IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	:	CASE NO. 1:08 CR 0510
Plaintiff,	:	
-vs-	:	MEMORANDUM OF OPINION AND ORDER DENYING THE DEFENDANT'S REQUEST FOR AN EVIDENTIARY HEARING AND DENYING THE DEFENDANT'S MOTION TO SUPPRESS
MARK SCHIMLEY,	:	
Defendant.	:	

UNITED STATES DISTRICT JUDGE LESLEY WELLS

Before the Court is a motion to suppress and a request for an evidentiary hearing, filed by defendant Mark Schimley. (Docket No. 23)(hereinafter "Defendant's Brief"). Mr. Schimley challenges the validity of a warrant executed at his home on 6 March 2007, at 1225 North Road, Apt. 110, Niles, Ohio, which authorized the search and seizure of fruits, instrumentalities, and evidence of crimes punishable under 18 U.S.C. § 2252. (Defendant's Brief at 1). The defendant maintains that issuance of the warrant was without probable cause, as the affidavit supporting it contained materially false and unreliable information. (Defendant's Brief at 1). Mr. Schimley specifically argues that he has made a substantial preliminary showing of intentional or reckless falsehood required under Franks v. Delaware, 438 U.S. 154 (1978), which would entitle him to an evidentiary hearing on the veracity of statements included in the affidavit. (Defendant's Brief at 2).

The government has filed a brief in opposition to Mr. Schimley's motion and argues that neither suppression of the evidence nor a Franks hearing are appropriate. (Docket No. 24)(hereinafter, "Brief in Opposition"). While the government concedes that the affidavit underlying the warrant contained two false statements, it maintains that the warrant is nonetheless valid, because the false statements were not "made knowingly and intentionally, or with reckless disregard for the truth." (Brief in Opposition at 1).

For the reasons stated herein, the Court will deny Mr. Schimley's request for an evidentiary hearing and will deny his motion to suppress.

I. Background

The warrant affidavit at issue in this case was based, in part, on the investigations of Trooper Robert Erdely of the Pennsylvania State Police ("Trooper Erdely" or "the trooper"), who had been tracking the distribution of child pornographic images and movies through peer-to-peer ("P2P") file sharing networks on the internet. (Brief in Opposition at 1-3). In order to make discussion of the warrant, the affidavit, and Trooper Erdely's investigative methods clear, the Court begins by providing relevant background on the use of P2P file sharing networks.

A. Peer to Peer Filing Sharing

P2P filing sharing networks provide a means by which one Internet user can share his or her digital files, including movies and photographs, with other internet users. (Docket 23-2 ¶14)(hereinafter "Affidavit"). After installing P2P software, an

internet user may join a network of other users running compatible P2P software. (Affidavit ¶14). The user may make his or her digital files available to others on the network, and, in turn, have access to those files that others wish to share. (Affidavit ¶14). The user is free to search the network by keyword for the types of files in which he or she is interested. (Affidavit ¶14). For instance, someone interested in obtaining child pornography might search for files using the keyword "preteen sex." (Affidavit ¶15). This keyword search would produce a list of all those files belonging to other users on the network, which contain that search term . (Affidavit ¶15). The user may select files from the list that he or she wishes to download, and the chosen files are downloaded directly from the computer or computers hosting the file. (Affidavit ¶15).

For the sake of speed and efficiency, the chosen file may come from multiple sources, with pieces of an image or movie coming from several computers on the network. (Affidavit ¶16). To ensure that the file reaches the correct destination, the P2P software identifies those computers involved in the transaction by reference to an Internet Protocol ("IP") address, which is a numeric identifier unique to each computer on the network. (Affidavit ¶¶6,15). Furthermore, the file itself contains a unique identifier known as a "SHA-1 Hash Value" or Secure Hash Algorithm-1, which, among computer forensics professionals, is considered the "fingerprint" of a file. (Affidavit ¶6(l); Brief in Opposition at 4).

B. Trooper Erdely's Investigation, the Warrant, and the Search and Seizure

On 13 February 2007, from the Area III Computer Crimes Task Force in Pennsylvania, Trooper Erdely conducted a search for child pornography using an internet connected computer and P2P software known as "Phex." (Affidavit at ¶23). The trooper's keyword search[1] produced a list of some 3929 files available for download from a computer with the IP address 24.166.103.205. (Affidavit at ¶23). Among them, he identified sixty movie and picture files that appeared to contain names relating to child pornography. (Affidavit at ¶23). Trooper Erdely then downloaded one suspect file from the IP address 24.166.103.205, which he reviewed and described as follows:

> a) [Loli Child Porn] (Loli Y) Babj 00(New) by Kidzilla.avi (video file of nude pre-pubescent female, with no pubic hair, stripping. An adult male is then seen penetrating the vagina of the prepubescent on multiple occasion [sic] during the twenty one minute (21 min) video clip. The prepubescent female is also seen using an oversized sharpie marker to penetrate her vagina).

(Affidavit at ¶23). It was later determined that, at the date and time the trooper downloaded the file, the IP address 24.166.103.205 was assigned to an account registered to the defendant Mark Schimley, at 1225 North Road, Apt 110, Niles, Ohio 44446. (Affidavit at ¶26). Furthermore, Trooper Erdely matched the unique SHA-1 hash value of the downloaded file with the file that was being shared at IP address 24.166.103.205, in order to confirm that they were one and the same. (Affidavit at

[1] According to the affidavit used to support the warrant, Trooper Erdely's search term was "[Loli Child Porn] (Loli Y) Babj00(New) by Kidzilla.avi," which is a commonly downloaded file on child pornography networks. (Affidavit at 23). This averment, however, was false, and the government concedes that Trooper Erdely had in fact searched using a different keyword associated with child pornography. (Brief in Opposition at 2). While the government's brief does not make entirely clear what the actual search term was, Mr. Schimley takes no issue with this discrepancy, and the Court sees no reason to consider the issue further.

¶24). Trooper Erdely also matched the SHA-1 hash values of the other 59 suspect files with video / image files encountered in other investigations, and identified them as videos known to depict minors engaged in sexually explicit conduct. (Affidavit at ¶25).

Armed with the trooper's findings, Special Agent Joseph Russ of the FBI ("Agent Russ" or "the agent") applied for a search warrant on 6 March 2007 for the property known as 1225 North Road, Apt. 110, Niles, Ohio 44446. (Brief in Opposition at 1). In support of the warrant, Agent Russ provided an affidavit reciting the details of Trooper Erdely's investigation. (Brief in Opposition at 1). Of particular importance here, Agent Russ attested that the trooper had downloaded a file entitled "[Loli Child Porn] (Loli Y) Babj00(New) by Kidzilla.avi" from the IP address registered to Mr. Schimley. (Affidavit at ¶23(a)). After reviewing the affidavit, the magistrate judge granted the warrant, having found probable cause for violations of 18 U.S.C. 2252. (Affidavit at 1). Agents subsequently searched Mr. Schimley's residence and seized his personal computer. (Defendant's Brief at 3).

A review of Mr. Schimley's computer revealed that the file referred to in Agent Russ's affidavit, "[Loli Child Porn] (Loli Y) Babj00(New) by Kidzilla.avi," was not present on the hard drive. (Defendant's Brief at 3). Furthermore, a forensic analysis indicated a strong likelihood that Mr. Schimley's computer had never contained a file with that name.[2] (Defendant's Brief at 8). However, agents did find a file entitled

[2] The forensic analysis conducted by Wayne A. Marney revealed that "no example of [the] file [was] present on the computer evidence." (Docket No. 23-2 at 25-26)(hereinafter "Marney Affidavit"). Mr. Marney found no fragments or artifacts of the file in program files, user registry hives, system restore points, or link files. (Marney Affidavit at ¶6). Mr. Marney further attested that it was unlikely that the file had simply been deleted or overwritten, as some remnant would still exist on Mr. Schimley's computer. (Marney Affidavit at ¶6).

"(Hussyfan)(pthc)(r@ygold)(babyshivid)Babyj Child abuse dark secret~Very willing premature sexualized little girls 3yo to 7yo shamed in pedofamilies.avi." (Brief in Opposition at 6). Although the government concedes that the name of the file found on Mr. Schimley's computer does not match the filename referenced in the affidavit, it maintains that this file is, in its substance, the very same movie file that Trooper Erdely downloaded from the defendant's IP address. (Brief in Opposition at 4-5). This was confirmed, the government insists, when Trooper Erdely matched the SHA-1 hash value of the downloaded file to the file being shared at Mr. Schimley's IP address. (Brief in Opposition at 5). Mr. Marney does note, however, that the SHA-1 hash value which would identify the file "[Loli Child Porn] (Loli Y) Babj00(New) by Kidzilla.avi," was not listed in the affidavit. (Docket No. 23-2 at 25-26, ¶7)(hereinafter "Marney Affidavit").

The government explains the discrepancy as a consequence of the process by which Trooper Erdely conducted his investigation using the Phex program. (Brief in Opposition at 4-5). According to the government, when a keyword search on Phex results in a list of files suspected to be child pornography, the unique SHA-1 hash values embedded in suspect files are cross-referenced with a text file which "contains the names and hash values of known child pornography images recovered from other investigations." (Brief in Opposition at 5). When there is a match between a suspect file and a file listed in the text file, Phex assigns the suspect file with the filename as designated by the text file. Essentially, the trooper's text file is a catalogue of titles and their corresponding unique hash values, against which downloaded files are compared. (Brief in Opposition at 5). As the government explains it, "if the search results include a file with the same name or hash value as a file stored in the text file, then the name from

the trooper's text file will be assigned to the image he selects for download." (Brief in Opposition at 5-6).

The government maintains that is exactly what happened in this case. (Brief in Opposition at 5-6). It explains that the affidavit referenced the file as "[Loli Child Porn] (Loli Y) Babj00(New) by Kidzilla.avi" simply because Phex had identified it as such, when Phex cross-referenced the downloaded file with the trooper's text file. (Brief in Opposition at 4-5). Furthermore, because Agent Russ was apparently unaware of or misunderstood the above recited process by which Phex assigns file names, he simply included the name of the file as it was presented to him by Trooper Erdely. (Brief in Opposition at 5).

Based on the discrepancy between the filename as referenced in the affidavit and the filename as it was discovered on the seized computer, Mr. Schimley now argues that the warrant was lacking in probable cause. Mr. Schimley specifically argues that Agent Russ intentionally or recklessly included a material false statement, which would entitle him to an evidentiary hearing under Franks v. Delaware.

The Court finds that Mr. Schimley has not made such a showing, for the reasons discussed below.

II. Law and Analysis

A defendant is entitled to an evidentiary hearing regarding the sufficiency of a warrant affidavit if he can satisfy a two-part test: (1) he must make a substantial preliminary showing that the warrant affidavit contained false statements that were made "knowingly and intentionally, or with reckless disregard for the truth," and (2) the

challenged statements must be necessary to a finding of probable cause. Franks v. Delaware, 438 U.S. 154, 155-56 (1978). "Warrant affidavits carry with them 'a presumption of validity,' and 'the challenger's attack must be more than conclusory' and must allege 'deliberate falsity or reckless disregard [on the part] of the affiant' " United States v. Stuart, 507 F.3d 391, 396 (6th Cir.2007) (quoting Franks, 438 U.S. at 171). If the defendant fails to make the substantial preliminary showing, the presumption of validity with respect to the challenged affidavit is not overcome and a Franks hearing is not required. Id. at 171.

Under Franks, the defendant is directed to "point out specifically the portion of the warrant affidavit that is claimed to be false; and [the allegations] should be accompanied by a statement of supporting reasons." Franks, 438 U.S. at 171. The only specific challenge offered by Mr. Schimley is directed at Agent Russ's averment that Trooper Erdely downloaded a file entitled "[Loli Child Porn] (Loli Y) Babj00(New) by Kidzilla.avi."[3] The government's stipulation that this portion of the affidavit is false leaves the Court with two questions under Franks: first, whether Agent Russ included the falsehood intentionally or with reckless disregard for the truth; and, second, whether the falsehood was necessary to the finding of probable cause.

Because the first question goes to Agent Russ's state of mind, the Court may infer "reckless disregard from circumstances evincing obvious reasons to doubt the veracity of the allegations." United States v. Whitley, 249 F.3d 614, 621 (7th Cir. 2001).

---

[3] Mr. Schimley seems to imply that Trooper Erdely's description of the downloaded file and the process by which it was acquired should be considered as part of a blanket challenge to the affidavit. (Defendant's Brief at 10). The Court, however, will only consider those portions of the warrant affidavit that Mr. Schimley has specifically challenged pursuant to Franks v. Delaware.

Courts are willing to make such an inference when presented with evidence that the affiant should have known that he was attesting to something that was false. For instance, in a case cited by Mr. Schimley, the court found that an officer acted recklessly when he admitted to having seen the defendant's criminal history yet included a false statement in the affidavit that was inconsistent with the defendant's record. United States v. Flake, 30 Fed. Appx. 736, 737-38 (9th Cir. 2002).

In the instant case, Mr. Schimley argues that the agent's actions were intentional or reckless by pointing out that the filename referenced in the affidavit was not present on Mr. Schimley's computer, and he further asserts that this discrepancy was confirmed by Mr. Marney's forensic analysis. In essence, Mr. Schimley argues that because Agent Russ included a false statement in the affidavit, he was necessarily reckless. However, Franks teaches that a mere showing of falsity is insufficient to demonstrate recklessness on the part of the affiant. Franks, 438 U.S. at 171-72. The facts asserted by Mr. Schimley provide evidence that Agent Russ's statement was in fact false, but they do not suggest that Agent Russ should have known it was so. Mr. Schimley does not offer facts like those presented in Flake, which would indicate that Agent Russ knew or should have known that the statement was false. He has therefore failed to make a substantial showing that the agent acted intentionally or recklessly when he included the falsehood in the affidavit. Furthermore, the file naming function of the Phex program and Agent Russ's reliance on Trooper Erdely's report tend to show that Agent Russ's inclusion of the wrong file name was not done intentionally or with reckless disregard for the truth.

Even if the Court were to accept that Agent Russ had acted intentionally or recklessly, it still would not grant the defendant's motion for a Franks hearing, as the specific false statement was not material to a finding of probable cause. Mr. Schimley's challenge to the filename is essentially an attack on nothing more than a label, the exclusion of which would do nothing to disturb the substance of the affidavit. The mislabeling of the file resembles those cases in which courts rejected challenges to affidavits where the affiant had misidentified an apartment or house number of a residence to be searched. For instance, in United States v. Warren, the court ruled that a warrant is not invalidated by an affidavit's erroneous reference to "apartment #1" when the residence to be searched was actually designated as "apartment B." United States v. Warren, 42 F.3d 647, 653 (D.C. Cir. 1994); See also State v. Taylor, 612 N.E.2d 728, 733 n. 2 (Ohio Ct. App. 1992) (holding that misstatement of house address in warrant affidavit was immaterial to probable cause determination). Like the misidentifications in these cases, the mislabeling of the file has no bearing on the question of probable cause.

Mr. Schimley has failed to make the required showing under Franks v. Delaware, which would entitle him to an evidentiary hearing. Therefore, the warrant is presumed valid.

III. Conclusion

For the foregoing reasons, the Court DENIES the defendant Mark Schimley's request for an evidentiary hearing and DENIES his motion to suppress.

IT IS SO ORDERED.

/s/ Lesley Wells
UNITED STATES DISTRICT JUDGE

Dated: 25 September 2009